ORACLE CONFIDENTIAL

"Express Mail" Mailing Label No. **EV 422226259US**

PATENT APPLICATION
ATTORNEY DOCKET NO. OR03-17301

UNITED STATES UTILITY PATENT APPLICATION

FOR

METHOD AND APPARATUS FOR FACILITATING SECURE CENTRALIZED ADMINISTRATION OF DATABASES

INVENTORS:

Daniel M. Wong and Min-Hank Ho

Oracle Corporation

500 Oracle Parkway

Redwood Shores, CA 94065

METHOD AND APPARATUS FOR FACILITATING SECURE CENTRALIZED ADMINISTRATION OF DATABASES

Inventors: Daniel M. Wong and Min-Hank Ho

BACKGROUND

Field of the Invention

[0001] The present invention relates to databases. More specifically, the present invention relates to a method and an apparatus for facilitating secure, centralized administration of databases.

Related Art

[0002] As technology becomes increasingly more affordable, and as the number of applications that collect and maintain data increases, there has been a corresponding increase in the number of databases and database servers that organizations utilize to manage data. With the increased number of databases and database servers comes the added burden of administering these servers. For large-scale organizations that maintain hundreds of databases, this can prove to be a daunting task. Moreover, as employees come and go and security policies change, the databases and database servers can easily fall out of compliance with

an organization's security policies, which can give rise to serious security vulnerabilities.

[0003] Enterprise organizations typically spend vast sums of money to ensure that all of their databases and database servers are up to date and are in compliance with an organization's policies. Traditionally, this involves employing a large number of database administrators who continually configure the databases and database servers to ensure compliance with the organization's policies. However, as the number of database administrators increases, so does the organization's potential vulnerability to a rogue administrator. Moreover, because database configuration operations are typically performed manually by administrators, the increased number of administrators results in an increased chance for human error.

[0004] Hence, what is needed is a method for configuring database servers without the problems listed above.

SUMMARY

[0005] One embodiment of the present invention provides a system that facilitates configuring a database. During operation, the system requests database configuration information from a directory server that stores configuration information for a plurality of database instances. In response to this request, the system receives the database configuration information, and configures the database in accordance with the database configuration information received from the directory server. This enables the database server to be configured without requiring manual configuration operations by a database administrator.

[0006] In a variation on this embodiment, the database is structured as a database server, and the database configuration information includes service-related settings for the database server.

[0007] In a variation on this embodiment, the database configuration information can include an audit trail, a security model, a security protocol parameter, a maximum sessions parameter, a database block size, an optimization mode parameter, and an OLAP features parameter.

[0008] In a variation on this embodiment, the database configuration information can include an Access Control List (ACL). This ACL identifies objects and services which are available on the database server, and also specifies which hosts have permissions to use the objects and the services.

[0009] In a variation on this embodiment, the directory server is Highly Available (HA).

[0010] In a variation on this embodiment, the system caches a local copy of the configuration information to facilitate configuration of the database when the database cannot connect to the directory server.

[0011] In a variation on this embodiment, the system receives a request for resources from a user at the database and determines if the user is an enterprise user. If so, the system queries the directory server for a user profile associated with the user and subsequently receives the user profile from the directory server. The system then allocates resources to the user based on parameters specified in the user profile.

[0012] In a further variation, the user profile can include a CPU quota for the user, a disk quota for the user, a scheduling priority for the user, and a read/write/execute permission for the user.

[0013] In a variation on this embodiment, the database configuration information can define a Security Admin (SA) role for the database.

[0014] In a variation on this embodiment, the database server periodically queries the directory server for updated database configuration information for the database.

BRIEF DESCRIPTION OF THE FIGURES

[0015] FIG. 1 illustrates a computing environment in accordance with an embodiment of the present invention.

[0016] FIG. 2 presents a flowchart illustrating the process of installing a database server in accordance with an embodiment of the present invention.

[0017] FIG. 3 presents a flowchart illustrating the process of granting access for resources to a user in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION

[0018] The following description is presented to enable any person skilled in the art to make and use the invention, and is provided in the context of a particular application and its requirements. Various modifications to the disclosed embodiments will be readily apparent to those skilled in the art, and the general principles defined herein may be applied to other embodiments and applications without departing from the spirit and scope of the present invention. Thus, the present invention is not intended to be limited to the embodiments shown, but is to be accorded the widest scope consistent with the principles and features disclosed herein.

[0019] The data structures and code described in this detailed description are typically stored on a computer readable storage medium, which may be any device or medium that can store code and/or data for use by a computer system. This includes, but is not limited to, magnetic and optical storage devices such as disk drives, magnetic tape, CDs (compact discs) and DVDs (digital versatile discs or digital video discs), and computer instruction signals embodied in a transmission medium (with or without a carrier wave upon which the signals are modulated). For example, the transmission medium may include a communications network, such as the Internet.

Computing Environment

[0020] FIG. 1 illustrates computing environment 100 in accordance with an embodiment of the present invention. Computing environment 100 includes network 102. Network 102 can generally include any type of wire or wireless communication channel capable of coupling together computing nodes. This includes, but is not limited to, a local area network, a wide area network, or a combination of networks. In one embodiment of the present invention, network 102 includes the Internet.

[0021] Coupled to network 102 are servers 104 and 110 to 114. Servers 104 and 110 to 114 can generally include any nodes on a computer network including a mechanism for servicing requests from a client for computational and/or data storage resources. Coupled to server 104 is database 108. Database 108 can include any type of system for storing data in non-volatile storage. This includes, but is not limited to, systems based upon magnetic, optical, and magneto-optical storage devices, as well as storage devices based on flash

memory and/or battery-backed up memory. Computing environment 100 also includes user 106 who interacts with server 104.

[0022] In one embodiment of the present invention, server 110 is a directory server that contains configuration information for database 108. This configuration information may include configuration information for the server 104 on which database 108 resides as well as configuration information for database 108. For example, directory server 110 may contain configuration information for database 108, including an audit trail, a security model, security protocol parameters, a maximum sessions parameter, a database block size, optimization mode parameters, and OLAP features parameters. This configuration information facilitates centralized management, unattended server and database installations, and user access to resources.

[0023] For example, as server 104 is installed, server 104 contacts directory server 110 via network 102 for configuration information pertaining to server 104 as well as configuration information for database 108 that is to be installed on server 104. This allows for server 104 and database 108 to be installed according to predefined policies with minimal or no input from user 106.

[0024] As users request resources on database 108, database 108 may query directory server 110 for access parameters for the requesting user. For example, as user 106 requests to gain access to resources controlled by database 108, database 108 may query server 110 for access information pertaining to user 106. This access information may include read/write/execute permissions for objects in database 108, a CPU quota for user 106, a disk quota for user 106, a scheduling priority for user 106, and a default profile for user 106.

[0025] Additionally, server 104 may keep a local cached copy of all configuration information received from directory server 110 to facilitate configuration and access control for times when directory server 110 may be unavailable.

[0026] Note that directory server 110 may be a standalone server, as well as a member of a cluster that includes servers 112 and 114. Aggregating configuration and security information for all databases and database servers within an organization at a directory server or a clustered directory server greatly reduces administration overhead as well as increases enterprise security. This allows for more servers to be configured, installed, and administered by fewer users which saves time and reduces potential security hazards.

Installing a Database Server

[0027] FIG. 2 presents a flowchart illustrating the process of installing database server 104 in accordance with an embodiment of the present invention. The system starts when database server 104 encounters a parameter to be configured for database server 104 (step 202). Next, database server 104 queries directory server 110 for configuration information for database server 104 (step 204). After receiving this configuration information, database server 104 configures the parameter with a value specified by the configuration information received from directory server 110 (step 206). Note that database server 104 may also cache a local copy of configuration information received from directory server 110.

Granting Access to Resources

[0028] FIG. 3 presents a flowchart illustrating the process of granting a user 106 access to resources in accordance with an embodiment of the present invention. The system starts when database 108 receives a request for resources from user 106 (step 302). In response to this request, database server 104 queries directory server 110 for all access configuration information pertaining to user 106 (step 304). Once the access configuration information is received, database 108 configures access permission for user 106 based on the received access configuration information (step 306). Note that user 106 may be a local user to database 108 who is unknown to directory server 110. In this case, database 108 may optionally access local configuration information not received from directory server 110. Note that additional variations and exceptions may be additionally defined through security policies on directory server 110.

[0029] The foregoing descriptions of embodiments of the present invention have been presented for purposes of illustration and description only. They are not intended to be exhaustive or to limit the present invention to the forms disclosed. Accordingly, many modifications and variations will be apparent to practitioners skilled in the art. Additionally, the above disclosure is not intended to limit the present invention. The scope of the present invention is defined by the appended claims.